Dienstvereinbarung

über die Einrichtung und den Betrieb elektronischer Schließsysteme

in den Gebäuden der Universität Regensburg

Zur Gewährleistung der schutzwürdigen Belange der Beschäftigten, insbesondere vor unzulässigem Gebrauch und unberechtigtem Zugriff auf Ihre personenbezogenen Daten, sowie zur Wahrung der berechtigten Interessen der Dienststelle schließen die Universität Regensburg, vertreten durch den Kanzler, und der Personalrat der Universität Regensburg, vertreten durch die Vorsitzende gemäß Art. 73 i.V.m. Art. 75 a Abs. 1 BayPVG folgende Dienstvereinbarung:

§1
Gegenstand und Geltungsbereich

Diese Dienstvereinbarung regelt den Einbau und den Betrieb neu zu installierender und bereits vorhandener elektronischer Schließsysteme in den Gebäuden und Räumen der Universität Regensburg. Sie gilt für alle betroffenen Beschäftigten der Universität Regensburg und für alle sonstigen Personen, die Zugang zu dem jeweiligen System oder dessen Daten haben.

§2
Zweckbestimmung

Elektronische Schließsysteme werden ausschließlich zur Verbesserung der Sicherheit für Personen, Anlagen und Gegenstände in den Räumlichkeiten der Universität Regensburg sowie zur effizienteren und wirtschaftlicheren Verwaltung von Zutrittsberechtigungen eingesetzt. Es ist untersagt, personenbezogene Daten im Hinblick auf die Erstellung von Anwesenheits- oder Bewegungsprofilen zu sammeln. Eine Leistungs- oder Verhaltenskontrolle der betroffenen Personen findet nicht statt.

§ 3
Betrieb der Anlagen

(1) Verantwortlich für den zentralen Betrieb der elektronischen Schließanlagen ist der Leiter der Technischen Zentrale. Für einzelne Gebäude können in Ausnahmefällen dezentrale Schließanlagen installiert werden.

(2) Vor Inbetriebnahme einer Schließanlage sowie bei wesentlichen Änderungen am System mit Auswirkungen auf Art und Umfang der Datenerhebung, -verarbeitung, -nutzung und/oder -speicherung ist bei dem Datenschutzbeauftragten eine datenschutzrechtliche Verfahrensbeschreibung einzureichen und eine Freigabe zu beantragen.

(3) Die Inbetriebnahme der Anlage darf erst nach der Freigabe durch den Datenschutzbeauftragten erfolgen. Ein Verstoß hiergegen muss die sofortige Außerbetriebnahme der Anlage zur Folge haben.

§4
Erfassung, Verwaltung und Auswertung von Daten

(1) Alle Beteiligten sind zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet. Vorgesetzte und Organisationsverantwortliche haben auf eine entsprechende Unterrichtung der Mitarbeiter hinzuwirken und die Einhaltung der einschlägigen Vorschriften anzuleiten und laufend zu überwachen.

(2) Erhebung von Daten
Es werden ausschließlich die unter Punkt 3 der jeweiligen Anlage zu den einzelnen Schließanlagen genannten Daten erfasst. Die mit einer Zugangskontrolle versehenen Räume sind unter Punkt 2 der jeweiligen Anlage gelistet.

(3) Nutzungsberechtigungen der Daten
Zugriff auf die personenbezogenen Daten haben lediglich die Personen, die als Administratoren des jeweiligen Schließsystems benannt sind. Sie sind unter Punkt 4 der jeweiligen Anlage gelistet. Die Daten sind vor unbefugtem Zugriff zu schützen.

(4) Auswertungen
Das Auslesen der Daten und/oder deren Auswertungen (sofern diese das jeweilige Schließsystem zulässt) nimmt die Universität nur bei sicherheitsrelevanten Ereignissen und Ereignissen von strafrechtlicher Relevanz vor. Das Auslesen aus den Schließzylindern und die Auswertung aus dem System erfolgt durch berechtigte Administratoren des Schließsystems in Anwesenheit eines Personalratsmitglieds nach Genehmigung durch den Kanzler im Einvernehmen mit dem Datenschutzbeauftragten. Die dabei gewonnen Daten sind nach Abschluss der Untersuchung, spätestens jedoch nach 14 Tagen, soweit sich keine weiteren Verdachtsmomente ergeben, datenschutzrechtlich konform zu löschen bzw. zu vernichten.

Die Administratoren des Schließsystems sind zudem berechtigt, Zutrittsberechtigungen und Zutrittsprotokolle auszulesen, wenn dies ausschließlich zu technischen Zwecken notwendig ist, wie z. B. bei Wartungsarbeiten, Fehlersuche, Sicherheitstests, Funktionstests. Der Personalrat ist grundsätzlich im Vorfeld über die Erforderlichkeit und die Durchführung von Auslesevorgängen und Auswertungen zu technischen Zwecken zu informieren, in begründeten Ausnahmefällen kann dies auch im Nachgang geschehen. Eine Weitergabe der gewonnen Daten und darauf basierenden Auswertungen an weitere Personen, die nicht unmittelbar mit der technischen Problemlösung betraut sind, erfolgt nicht. Nach Abschluss der technischen Maßnahmen, spätestens jedoch nach 14 Tagen sind die gewonnen Daten und darauf basierenden Auswertungen datenschutzrechtlich konform zu löschen bzw. zu vernichten. Eine längere Aufbewahrung zur technischen Problemlösung ist mit der Zustimmung von Datenschutzbeauftragtem und Personalrat in Ausnahmefällen möglich. Auf die Sonderregelungen zu den einzelnen Schließsystemen aufgrund der Anlagen wird hingewiesen.

Eine Verknüpfung des Schließsystems einschließlich seiner Daten mit anderen als in der Anlage genannten EDV-Systemen oder Dateien bedarf der erneuten Freigabe und vorherigen Zustimmung des Personalrats.

Sofern bei Wartungs- und Reparaturarbeiten an dem elektronischen Schließsystem den damit beschäftigten Personen Informationen bekannt werden, die gemäß dieser Dienstvereinbarung oder anderen Bestimmungen vertraulich zu behandeln sind, haben sie über den Inhalt Stillschweigen zu bewahren, ebenso über die Erkenntnisse, die Rückschlüsse auf das Verhalten der Systemanwender zulassen könnten.

(5) Schlüsselnutzung
Die Mitarbeiter/innen sind verpflichtet, mit Schlüsseln oder anderen Zugangsmitteln (z.B. Passwörtern) sorgsam umzugehen und einen etwaigen Schlüsselverlust sofort dem Administrator der Schließanlage (genannt in der jeweiligen Anlage zu dieser Dienstvereinbarung) zu melden.

§5
Rechte des Personalrats

(1) Der Personalrat hat das Recht, die Einhaltung dieser Dienstvereinbarung zu überprüfen. Hierzu erhält er auf Wunsch Einsicht in alle mit dem Betrieb des Systems zusammenhängenden Unterlagen, Protokolle und sonstige Aufzeichnungen.

(2) Der Personalrat kann nach vorheriger Information der Dienststelle Besichtigungen vor Ort vornehmen.

(3) Zur Überprüfung der Arbeitsweise des Systems darf der Personalrat mit der Dienststellenleitung Fachleute zu Rate ziehen.

(4) Bei Einführung, Inbetriebnahme und Änderungen ist nach Art. 75 a BayPVG der Personalrat mit einzubeziehen.

§6
Bekanntmachung der Dienstvereinbarung

(1) Diese Dienstvereinbarung ist allen betroffenen Personen zugänglich zu machen.

(2) Die Administratoren des jeweiligen Schließsystems werden zur Einhaltung dieser Dienstvereinbarung schriftlich verpflichtet.

§7
Inkrafttreten und Geltungsdauer

(1) Diese Dienstvereinbarung tritt am Tage ihrer Bekanntmachung in Kraft. Sie kann mit einer dreimonatigen Frist zum Ende eines Kalendervierteljahres gekündigt werden. Bis zum Abschluss einer neuen Dienstvereinbarung gilt die bisherige Dienstvereinbarung weiter, soweit nicht andere Rechtsvorschriften dem entgegenstehen oder die Parteien sich auf eine vorläufige Regelung einigen.

(2) Änderungen und/oder Erweiterungen einer bestehenden elektronischen Schließanlage oder die Beschaffung zusätzlicher Schließanlagen bedürfen der vorherigen Zustimmung des Personalrats.

(3) Für jedes elektronische Schließsystem gibt es eine Anlage zu dieser Dienstvereinbarung in der die jeweiligen Betriebsparameter festgehalten werden. Diese Anlagen sind Bestandteil der Dienstvereinbarung.

(4) Die Anhänge und deren Anlagen können auch ohne Kündigung der Dienstvereinbarung mit Zustimmung des Personalrats geändert werden; die Beteiligungsrechte der Mitarbeitervertretung bleiben hiervon unberührt.

Regensburg, 03.06.2016

Universität Regensburg

Dr. Christian Blomeyer
Kanzler

Regensburg, 07.06.2016

Personalrat

Ines Bauer
Vorsitzende

Anlage A
Schließanlage IKON+CliQ, Teststellung am Lehrstuhl für Medieninformatik

1. Systembeschreibung

1.1 Hardware

Als Türschlüssel dienen sogenannte **Transponder**. Diese sehen aus wie konventionelle mechanische Schlüssel, tragen jedoch zusätzlich einen elektronischen Chip, auf dem die jeweilige Schließberechtigung gespeichert ist. Der Transponder verfügt über eine Batterie zur Stromversorgung. Die Programmierung der Transponder erfolgt am Arbeitsplatz des Administrators.

Die **Schließzylinder** in den Türen sehen äußerlich wie konventionelle Schließzylinder aus. Sie enthalten ebenfalls einen elektronischen Chip, der einen Schließvorgang freigibt, wenn ein Transponderschlüssel in den Zylinder gesteckt wird und dessen Chip den passenden Code übermittelt. Die Schließzylinder enthalten keine Batterien, die Stromversorgung des Chips erfolgt über den Transponder. Der Chip speichert ebenfalls die Schließberechtigungen, zusätzlich wird gespeichert, welche Transponder die letzten 50 Schließvorgänge durchgeführt haben.

Die Programmierung der Schließzylinder erfolgt durch einen **Programmierschlüssel**. Dieser Schlüssel wird am Arbeitsplatz des Administrators programmiert. Anschließend wird er in den zu programmierenden Schließzylinder gesteckt und überträgt dann die Schließberechtigungen auf den Chip im Schließzylinder. Dieser Programmierschlüssel steht dem Systemadministrator zur Verfügung. Ein zweiter Programmierschlüssel verfügt zusätzlich über die Berechtigung, die letzten 50 Schließvorgänge an einem Schließzylinder auszulesen. Dieser Programmierschlüssel befindet sich i.d.R. an einem gesicherten Ort und kommt nur in Ausnahmefällen nach dem Vier-Augen-Prinzip (Auslesung bzw. Auswertung erfolgt durch den berechtigten Administrator des Schließsystems in Anwesenheit eines Personalratsmitglieds nach Genehmigung durch den Kanzler im Einvernehmen mit dem Datenschutzbeauftragten) zum Einsatz.

1.2 Software

Für die Programmierung und Verwaltung der Transponder sowie zum Auslesen von Daten aus den Schließzylindern kommt die Software „IKON+CLIQ CS04"in der Standardversion zum Einsatz. Die Software speichert, welcher Transponder an welche Person ausgegeben wird, welcher Transponder welche Schließzylinder sperrt und (falls diese Daten ausgelesen werden) welcher Transponder einen Schließzylinder gesperrt hat (max. 50 Vorgänge). Die Software wird auf den Rechnern des Administrators und des Lehrstuhlsekretariats lokal installiert, die Daten werden auf einem Server gespeichert. Der Zugang zu den Daten ist durch Passwort geschützt. Zugang zu den Protokolldaten der Schließvorgänge ist ausschließlich den Administratoren zum Zwecke der technischen Konfiguration und zur Kontrolle der Funktionsfähigkeit der Anlage vorbehalten (§ 4 Abs. 4).

2. Liste der betroffenen Räume

- PT 3.0.14 – Büro
- PT 3.0.27/-28 Future Interaction Lab
- PT 3.0.30 – Büro
- PT 3.0.31 – Büro
- PT 3.0.32 – Büro
- PT 3.0.44 – Büro
- PT 3.0.89 Treppenhaus

3. Liste der erfassten Daten

Datentyp	Grund für die Speicherung
Vorname Nachname Personen-ID Transpondernummer Transponder ausgegeben am Transponder zurückgegeben am	Transponderverwaltung und Zugangsberechtigung
Datum Uhrzeit Transpondernummer	Protokollierung der 50 letzten Schließvorgänge
Transpondernummer Schließberechtigungen (Raumnummern) -keine Verknüpfung mit Personendaten-	Transponderverwaltung und Zugangsberechtigung

4. Liste der Personen, die Zugang zu den Daten haben

- Hr. Raphael Wimmer (Systemadministrator), Mitarbeiter am Lehrstuhl für Medieninformatik
- Hr. Alexander Bazo (stv. Systemadministrator), Mitarbeiter am Lehrstuhl für Medieninformatik
- Sekretariat (Frau Ingrid Stitz) des Lehrstuhls für Medieninformatik

5. Speicherung von erhobenen Daten

In Abweichung von § 4 Abs. 4 Satz 3 der Dienstvereinbarung werden nur die im Rahmen der Erhebung gewonnenen personenbezogenen Daten und die darauf basierenden Auswertungen nach Abschluss der technischen Maßnahmen, spätestens jedoch nach 14 Tagen, datenschutzrechtlich konform gelöscht bzw. vernichtet. Während der Testphase können anonymisierte Daten über einen längeren Zeitraum genutzt werden. Diese Analysen dienen der späteren Systemauswahl.

6. Schlussbestimmungen

Diese Anlage der Dienstvereinbarung gilt für den Probebetrieb der **Schließanlage IKON+CliQ** zunächst für 24 Monate und wird vor Ablauf der Probephase erneut verhandelt und gegebenenfalls sofort im Anschluss neu abgeschlossen.

Regensburg, 03.06.2016

Universität Regensburg

Dr. Christian Blomeyer
Kanzler

Regensburg, 07.06.2016

Personalrat

Ines Bauer
Vorsitzende